AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information Associated With the Account
aegbinola@gmail.com
That is Stored in Premises Controlled by Google LLC

Case No. 3:19-sw- 324

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated fully by reference herein

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated fully by reference herein

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1343, 1349 and 1956(h)	Wire Fraud; Conspiracy to Commit Wire Fraud; and Conspiracy to Commit Money Laundering

The application is based on these facts:

See Affidavit

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of ____ days (give exact ending date if more than 30 days: May 13, 2020 is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI Special Agent Michael P. French
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/15/2019

/s/
David J. Novak
United States District Judge
Judge's signature

City and state: Richmond, Virginia

Honorable David J. Novak, U.S. District Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **AEGBINOLA@GMAIL.COM** THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 3:19SW324 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Michael P. French, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google LLC (hereafter "Google"), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a special agent (SA) with the Federal Bureau of Investigation (FBI) and, as such, I am charged with enforcing all federal laws in all jurisdictions of the United States, its territories and possessions. I have been employed as an FBI SA since September 2004. I have

extensive experience investigating all types of computer crimes including criminal and national security computer intrusions, child pornography, intellectual property rights violations, and theft of trade secrets. As an FBI SA I have received extensive training in the investigation of violations of federal and state law. I am currently assigned to the Richmond Division of the FBI where I investigate cyber matters, which include computer-enabled criminal violations relating to computer enabled fraud designed to induce victims to wire money to criminally controlled bank accounts.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of federal criminal law, specifically wire fraud (18 U.S.C. § 1343); conspiracy and attempt to commit wire fraud (18 U.S.C. § 1349); and money laundering conspiracy (18 U.S.C. § 1956(h)), have been committed by the person in control of the email address **aegbinola@gmail.com**. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTORY PROVISIONS

6. Title 18, United States Code, Section 1343 (wire fraud) provides:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

7. Conspiracy to commit wire fraud, as set forth in 18 U.S.C. § 1349, provides in pertinent part:

> Any person who attempts or conspires to commit [wire fraud] shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

8. Money laundering as set forth in 18 U.S.C. § 1956(a) is described in pertinent part as follows:

> (a)(1) Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—
>
> > (A)(i) with the intent to promote the carrying on of specified unlawful activity; *or*
>
> * * *
>
> (b) knowing that the transaction is designed in whole or in part—
>
> > (i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity;
>
> * * *

shall be sentenced to a fine of not more than $500,000 or twice the value of the property

involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both.

9. Title 18, United States Code, Section 1956(h) provides that "[a]ny person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy."

PROBABLE CAUSE

10. On or about September 26, 2018, an individual using the name "Rachel Moore" contacted an employee in the procurement department of a Virginia university using the email address accounts@kjellstromleegroup.com. As detailed further below, the accounts@kjellstromleegroup.com is very similar to the actual email domain name for Kjellstrom and Lee, which is a large construction company located in Richmond, Virginia, and which has completed construction projects for multiple universities, including the same Virginia university. "Rachel Moore" advised the procurement department employee that the bank account on file for receiving payments was currently being audited and inquired if the next payment could be sent to their foreign bank account. The university employee responded to "Rachel Moore" on September 28, 2018, with questions regarding the length of the audit and informed "Rachel Moore" that the university Treasury Department could assist her with setting up ACH transfers.

11. On October 4, 2018, "Rachel Moore" sent a reply email to the university employee stating:

> "Hope you are good. Thank you for the reply. In regards to the ACH setup, we can only have this done after the audit. The audit is usually between 4 and 6 weeks. Our CFO advised if we can have our payments sent by wire, and we setup

> the ACH once the audit is over. Will this be a possibility? Kindly get back to me as soon as you can. Thank you for your time."

The university employee responded to "Rachel Moore" on the same day and told "Moore" to contact the university once the audit was complete to get assistance with setting up ACH wire transfers. They further advised "Moore" that a form is required to setup ACH transfers and it would need to be sent to the university Treasury Department as they are the ones who enter the account information into the payment system.

12. On October 24, 2018, "Rachel Moore" contacted the university and asked, "Hope you are good. Do you have any payment for us?" The university employee responded on October 25, 2018 by stating, "The last payment I am showing in our system, was issued on check 31499151, in the amount of $1,401,569.76. If you have any open invoices, please email them to me. Thank you!"

13. On October 30, 2018, "Rachel Moore" sent a message to the university employee stating:

> Can you please confirm when check 31499151 was issued or sent out. In regards to the audit, we need to confirm what month to apply the payment to, in terms of when it was received. Thank you for your time.

On the same day, the university employee responded with a screenshot from the payment processing system showing the details of the most recent transaction.

14. Later, on October 30, 2018, "Rachel Moore" sent a follow-up message to the university employee that stated:

> Thank you for the information. We have not signed up to receive ACH payments yet, as we still have the audit ongoing, so please kindly notify us before our next payment is issued. Thank you for your time.

The university employee responded to "Rachel Moore" and asked if there were currently any

open orders with the university as there were currently no pending payments for their account.

15. On November 1, 2018, the university employee sent a follow up message to "Rachel Moore" stating, "There is a payment scheduled for today's check run. A check number has not been assigned as of yet, but the amount is $607,061.17. Reference number EP250XXXX."

16. On December 10, 2018, "Rachel Moore" sent the following message to the university employee:

> Hope you are good. We signed up for ACH a couple of weeks ago, but a remittance email was not requested. Can you please notify us at remittance@kjellstromleegroup.com when a payment has been made. Can you please also confirm our last payment was on the 1st of November. Thank you.

The university employee responded on December 11, 2018, and stated, "Check 3150XXXX was issued on 11-16-18, in the amount of $660,259.31. ACH was set up on 11/20/18; therefore, future payments will be sent directly to your account. Thank you!"

17. On December 20, 2018, the university initiated a payment via ACH wire transfer in the amount of $469,819.49 from their bank account to an account with the Bank of Hope, as listed in the ACH setup form provided by "Rachel Moore." On January 3, 2018, the university was contacted by their bank, which was concerned the December 20, 2018 wire transfer was fraudulent. The university contacted Kjellstrom and Lee and learned they did not have an employee named "Rachel Moore" and that no establishment of ACH wiring had been initiated by Kjellstrom and Lee.

18. The majority of the above-described $469,819.49 wire transfer could not be recovered and was a loss for the Virginia university. A trace of the proceeds of the $469,819.49 wire transfer revealed that after the money was deposited in the Bank of Hope account it was

quickly redistributed to multiple different banks via 13 different wire and check transactions over a three-day period from December 21 to December 24, 2018. This information, combined with evidence that the same perpetrators are suspected of registering over 50 Internet domains that are deceptively named to appear to belong to legitimate businesses, resulted in this Court issuing an ECPA search warrant for the Internet service provider, NameCheap, on February 12, 2019, case number 3:19-sw-52.

19. As part of the FBI's investigation into this wire fraud, on February 12, 2019, this Court issued a search warrant, case number 3:19-sw-51, pursuant to Rule 41(b)(6)(A), to allow the FBI to deploy a Network Investigative Technique (NIT) to the email address accounts@kjellstromleegroup.com. On February 15, 2019, the individual accessing the email account accounts@kjellstromleegroup.com opened the email message containing the NIT and the code contained in the attached file executed, providing a variety of data to an FBI controlled server, which included the IP address of the computer opening the attachment. This IP address of the computer was 86.191.189.88, which is owned by British Telecom (BT) in the United Kingdom.

20. According to information provided by the United Kingdom, the IP address 86.191.189.88 on February 15, 2019, at the time the NIT was executed was assigned to the subscriber Samiat Egbinola, address 56, Francisco Close, Chafford Hundred, Essex, RM16 6YD with BT customer ID of BBEU16104626. Also identified as residing at the residence was Olabanji O Egbinola. Egbinola was previously arrested in the United Kingdom in 2008 for money laundering. At the time of his arrest, a large quantity of US currency was seized from his residence and he was in possession of a computer with information on dozens of bank accounts of individuals who were victims of fraud. A review of Olabanji Egbinola's bank account showed

there was an expected annual income of £65,000 per year but there were no regular sources of income identified. The account is predominately funded by cash deposits that are quickly dispersed which is indicative of a money laundering technique known as layering.

21. A review US government records showed Olabanji Egbinola's travel to the US in 2016 where he provided a personal email address of aegbinola@gmail.com, which is the subject account of this search warrant. Olabanji Egbinola traveled to Los Angeles, California, in April 2015 and provided a destination address in Los Angeles that is associated with the subject of an FBI investigation for fraud and money laundering for schemes similar to the one being investigated by your affiant. Olabanji Egbinola also traveled to Los Angeles, California, again in July 2019 and provided a destination address of a Los Angeles-based hotel that is approximately two miles from the address he visited in 2015.

22. According to Google records, the email account aegbinola@gmail.com was registered on May 16, 2008, from a BT IP address located in the UK. The following Google services were subscribed to by Olabanji Egbinola:

1) Android, 2) Android Market, 3) Gmail, 4) Google AdSense, 5) Google Bookmarks, 6) Google Calendar, 7) Google Chrome Sync, 8) Google Docs, 9) Google Drive, 10) Google Hangouts, 11) Google Maps, 12) Google Notebook, 13) Google Payments, 14) Google Photos, 15) Google Play, 16) Google Services, 17) Has Madison Account, 18) Location History, and 19) YouTube.

23. A review of the email headers contained in the email account showed numerous communications with multiple individuals, including with the email address johnedwards79@yahoo.co.uk. This email address is associated with subject of another FBI investigation, who is a named defendant in a sealed indictment in the Western District of North

Carolina, for a similar fraud scheme targeting victims using spoofed domains of construction companies. Specifically, the johnedwards79@yahoo.co.uk was used to receive invoices for VPN ("virtual private network") services that the fraudsters used to hide their true IP address information while committing the fraud scheme. Additionally, the same account was used to receive information about construction companies that was later used to create spoofed domain names that were intrinsic to the fraud scheme. Messages between aegbinola@gmail.com and johnedwards79@yahoo.co.uk were exchanged multiple times over a period of several years. The defendant under indictment in the Western District of North Carolina is associated with a company named Florian London, which is based in the UK. Olabanji Egbinola listed Florian London as his employer on his travel documents when entering the United States in July 2019.

BACKGROUND CONCERNING GMAIL

24. In my training and experience, I have learned that Google provides a variety of online services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name Gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Gmail users) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

25. A Gmail user can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google.

26. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

27. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

28. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins

to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

29. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

30. In general, an email that is sent to a Google Gmail user is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

31. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or

control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.[1]

32. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

33. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. Email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the

[1] After passage of the CLOUD Act in March 2018, which is codified in 18 U.S.C. § 2713, providers subject to U.S. service are required to disclose records regardless of whether they choose to store their data in the U.S. or overseas.

account user at a particular time (*e.g.*, location information integrated into an image or video sent via email).

34. Lastly, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

35. Based on the forgoing, I respectfully submit that there is probable cause to believe that the email address described in Attachment A was used to further a criminal scheme or artifice to defraud, and I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Michael P. French
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on November 15, 2019

/s/
David J. Novak
United States District Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information and documentation associated with **aegbinola@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the "Provider" and/or "Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, *regardless of whether such information is stored, held or maintained inside or outside of the United States*, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, device information, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including : full name, user identification number, birth date, gender,

contact e-mail addresses, Google passwords, Google security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;

e. All records or other information pertaining to Google search history conducted by an individual using the account;

f. All records or other information containing historical location data maintained by Google associated with the account including GPS, Cellular, WiFi, or other in the custody or control of Google;

g. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

h. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

i. All "check ins" and other location information;

j. All documents, spreadsheets, photos or other files stored in Google Documents, Google Drive, or Google Photos

The Provider is hereby ordered to disclose the above information to the government within **14 days** of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §§ 1343, 1349 and 1956 involving the individual(s) using the email address **aegbinola@gmail.com** and occurring from the date of the

account's opening, to include, for each account or identifier listed in **Attachment A**, information pertaining to the following matters:

a. Email communications and all content (intrinsic, embedded, or attached) related to fraud and related activity in connection with computers, Internet fraud schemes, any conspiracy to commit the aforementioned violations, or any other fraud activity. Communications between the email address aegbinola@gmail.com and any other individuals/accounts who may have wittingly or unwittingly played a role in assisting the scheme to defraud described above;

b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

e. The identity of any person(s) who have communicated with the target email address or shared documents or files about matters relating to money laundering and/or Internet fraud, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, and my official title is _____. I am a custodian of records for Google. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google; and

c. such records were made by Google as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature